International Journal of Pure and Applied Researches http://ijopaar.com; 2020 Vol. 1(1); pp. 21-26, ISSN: 2455-474X

CUBIC AND QUADRATIC EQUATIONS WITH RESPECT TO GALOIS GROUP THEORY

Dr. Rajiva Dixit

Department of Mathematics,

B. S. N. V. P. G. College, Lucknow, U. P., India

Email: dixit.rajiva@gmail.com

Abstract

The process of forming Galois groups of polynomials is inseparable from degrees 3 and 4 over non-character 2 fields will be illustrated. It will be used by third and fourth degree mathematicians. Mathematics for these degrees will not be solved. Permissions and automorphisms will not be used.

1. Introduction

Let K be a field and f (x) be a separable polynomial in K[x]. The Galois group of f (x) over K permutes the roots of f(x) in a splitting field.
The roots r_1 , r_2, ….., r_n provide the construction of Galois group. The following two theorems without proof will be used for our help;

Theorem 1.1 Let f (x) over field K [x] be a separable polynomial of degree n

(a) If the polynomial f(x) is irreducible in K[x] then the Galois group over K has Order divisible by n.

(b) The polynomial f (x) is irreducible in L[X] if and only if its Galois group Over K is a transitive subgroup of S_n (symmetric group)

. **Definition: 1. 2** The discrminants of the following types of 3rd and 4th degree Equations are:-

$X^3 + a X + b = 0$ disc $(- a^3 - 27 b^2)$

$X^4 + a X + b = 0$ disc $(-27 a^4 + 256 b^3)$

$X^4 + a X^2 + b = 0$ disc $16 b (a^2 - 4 b)^2$

Galois Group of Cubic Polynomials

The Galois group of a cubic polynomial is completely determined by its determinant.

Method :

Let K (field of not characteristic 2) and f (x) be a separable irreducible cubic in K[X]. If disc f = square in K then the Galois group of f (x) over K is A_3
(alternating group; group of even permutations) If disc ≠ square in K then the Galois group of f (x) over K is S_3 (symmetric group of order 3 , 6 permutations)

The permutation action of the Galois group of f (x) on its roots turns the Galois group into a transitive subgroup of S_3 (theorem 1 .1). The only transitive subgroups of S_3 are A_3 and S_3. Our purpose is to find the transitive subgroups A_3 and S_3 of cubic equation using the discriminant of the given equation. For example:
In table-1 we list the discriminants and Galois groups over Q of the cubic equation $X^3 - a X - 1 = 0$ where $1 \leq a \leq 0$. We will discuss only irreducible polynomial. We will not discuss $x^2 - 2 x - 1 = 0$ because it is reducible.

f(x)	disc f $= - 4 a^3 - 27 b^2$	Galois group
$X^3 – X – 1$	-23 (not square)	S_3 ……(1)
$X^3 - 3 X - 1$	$81= 9^2$ (square)	A_3 ……..(2)
$X^3 - 4 X - 1$	229 (not square)	S_3 ……..(3)
$X^3 - 5 X - 1$	473 (not square)	S_3 ……(4)
$X^3 - 6 X - 1$	837 (not square)	S_3 ……..(5)
$X^3 - 7 x + 7$	7^2 (square)	A_3 ……..(6)

If a cubic polynomial has Galois group A_3 as in (2) , its roots all generate the same field extension of Q. So all the roots are real since at least one root is real. But if all the roots are real the Galois group does not have to be A_3 for example the polynomial:
$x^3 - 4 x - 1$
has all the real roots but its Galois group over Q is S_3. Each root of $x^3 – 4 x – 1$ generates a different cubic field in R .

Remarks 2.3 The cubics $x^3 - 2x + 1$ and $x^3 - 7 x - 6$ have discriminants 5 and $400 = (20)^2$, but this does not mean by theorem (2.1) that their Galois groups over Q are S_3 and A_3 both polynomials are reducible such that

$X^3 – 2x + 1 = (x – 1) (x^2 + x - 1)$ and

$X^3 - 7x - 6 = (x +1)(x + 2)(x – 3)$

First of all we must check that a cubic is irreducible before we apply theorem 2.1.
Secondly you must also check that it is separable if you are working in characteristics 3
Outside characteristics 3, irreducible cubics are automatically separable.

Example 2.4 Let F be a field and u be transcendental over F .
In F(u) [X] , the polynomial $x^3 + u x + u$ is irreducible by Eisentein' s criteria at u .
The discriminant is

$$- 4 u^3 - 27 u^2 = - u^2 (4 u + 27)$$

If F does not have characteristics 2 or 3, then this has a simple linear factor 4 u + 27. So the discriminant is not a perfect square . If F has characteristic 3, the discriminant is $– 4 u^3 = -$

u^3, which is not a perfect square . Therefore, when F does not have characteristic 2 the Galois group of $x^3 + u x + u$ over F (u) is isomorphic to S_3.

Is nice to have the record of few irreducible cubics over Q whose Galois group is A_3. In the following table 2 where each discriminant is a perfect square The polynomials in the table are all irreducible over Q since ± 1 are not roots or because they are all irreducible mod 2. We list all three roots of each cubic in terms of one root we call r. That list of roots is essentially telling us what the three elements of Gal(Q(r) / Q) are , as each automorphism is determined by its effect on r .

f (x)	disc f $= -4a^3 - 27b^2$	roots
$x^3 - 3x - 1$	9^2	$r,\ r^2 - r - 2,\ -r^2 + 2$
$x^3 - x^2 - 2x + 1$	7^2	$r,\ r^2 - r - 1,\ -r^2 + 2$
$x^3 + x^2 - 4x + 1$	(13^2)	$r,\ r^2 + r - 3;\ -r^2 - 2r + 2$
$x^3 + 2x^2 - 5x + 1$	$(19)^2$	$r,\ r^2 + 2r - 4,\ -r^2 - 3r + 2$

Table 2 Some cubics with Galois group A_3 over Q

GALOIS GROUP OF QUADRATICS

To compute Galois groups 0f separable irreducible quadratics (4^{th} degree polynomials) We first list the permutations of symmetric group S_4 then the transitive subgroups of S_4 . These are candidates for the Galois groups by theorem 1.1.

PERMUTATIONS OF SYMMETRIC GROUP S_4

PERMUTATIONS	TYPE
(12) , (13) , (14) , (23) , (24) , (3 4)	2 CYCLES
(12)(34) , (13)(24) , (14)(23)	PRODUCT OF 3 – CYCLES
(123) , (124) , (1 3 2) , (134) , (1 4 2) , (143) , (23 4) , (243)	3 – CYCLES
(1234) , (1243) , (1324) , (1342) , (1423) , (1432) .	4 – cycles

There are 30 subgroups of S_4 . Which are displayed in the following table, except e and S_4 . There elements are given in the following table.

Elements	Order	Isomorphic to
{ e , (12)(34) , (13)(24) , (14)(23) , (123) , (124) ……. … (132) , (134) , (142) , (143) , (234) , (243) }	12	A_4
{ e , (12)(34) , (13)(24) , (14)(23) }	4	V_4

{ e , (12)(34) } , { e , (13 (24) }, { e , (14)(23) }	2 , 2 . 2	Z_2
{ e , (123) , (132) }	3	Z_3
{ e , (124) , (142) }	3	Z_3
{ e , (134) , (143) }	3	Z_3
{ e , (234) , (243) }	3	Z_3
{ e , (12) , (12)(34) , (13)(24) , (14)(23) , (34) , (1324) , (1423) }	8	D_4
{ e, (12)(34) , (1324) , (1423) }	4	Z_4
{ e , (12)(34) , (13(24) , (14), (14)(23) , (23) , (1243) , (1342) }	8	D_4
{ e , (14)(23), (1243) , (1342)}	4	Z_4
{ e , (12) , (13), (23) , (123) , (132) }	6	S_3
{ e , (12), (14) , (24) , (124) , (142) }	6	S_3
{ e , (13) , (14) . (34) , (134) , (143) }	6	S_3
{ e , (23) , (24) , (34) , (234) , (243) }	6	S_3 .
{ e , (12) , (12)(34) . (34) }	4	V_4
{ e , (12) } , { e , (34) }	2 , 2	Z_2
{ e , (13) } ,{ (13) (24) , (24) }	4	V_4
{e , (13) } , { e , (24) }	2 , 2	Z_2
{ e , (14) , (14)(23) , (23) }	4	V_4
(e , (14 } , { e , (23) }	2 . 2	Z_4

The treatments of Galois groups of cubic and quadratic polynomials usually avoid fields of characteristics 2. Here we will discuss these Galois groups of all characteristics. Here we will refer two theorems, which will be used in the treatment of Galois groups of all characteristics.

Theorem 1 : Let K not having characteristics 2 and f(X) be a separable irreducible cubic in K[X] . If discf = □ (square) in K then the Galois group of f (X) over K is A_3 If discf ≠ □ (square) in K then the Galois group of f (X) over K Is S_3.
(Problems concerning to this theorem have solved above)
Theorem 2: Let K not have characteristic 2 and

$$f(X) = X^4 + aX^3 + bX^2 + cX + d$$

be irreducible in K [X] . The Galois group G_f of (X) over K can be described in terms of whether or not its discriminant is a square in K and whether or nor its cubic resolvent

$$R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd)$$

factors in K [X] , accordingly in the following table .

disc f	$R_3(X)$ in K [X]	G_f (Galois) isomorphic to
≠ □ (square)	irreducible	S_4
= □ (square)	irreducible	A_4
≠ □ (square)	reducible	D_4 or Z / 4Z
= □ (square)	reducible	V

Now we are concerned with quadratic polynomials and find the Galois group. (field K will not have characteristic 2) , more than 2 ;

The following definition or formula will be frequently used when dealing with quadratic polynomials.

Definition : - When f (X) is quadratic with roots r_1 , r_2 , r_3 , r_4 , its cubic resolvent $R_3(X)$ is the cubic polynomial

When f (X) is monic , we have the $R_3(X)$

$$R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd)$$

This may or may not be irreducible over K.

It is useful to record a special case of the cubic resolvent . Let a = b = 0, then $f(X) = X^4 + cX + d$ => $R_3(X) = X^3 - 4dX - c^2$.

Example 1: We compute the Galois of $X^4 - X - 1$ over Q . This polynomial is irreducible over Q since it is irreducible mod 2 . ;
The cubic resolvent of $X^4 - X - 1$ is $X^3 + 4X - 1$ which is irreducible over Q . (± 1 are not its roots) . That shows the splitting field of $X^4 - X - 1$ contains a cubic subfield (namely $Q(r_1r_2 + r_3r_4)$) , so the Galois group of $X^4 - X - 1$ over Q has order divisible by 3 . The splitting field also contains

$Q(r_1)$, so the Galois group is also divisible by 4. Therefore the Galois group is also divisible by 4. Therefore the Galois group is either A_4 or S_4.

The discriminant of $X^4 - X - 1$ is -283, which is not a perfect square, so the Galois group must be S_4.

Example 2: Now we find the Galois group of $X^4 + 8X^2 + 12$ over Q.
First we show that the polynomial is irreducible. If it is reducible then it has a linear factor or it is product of two quadratic irreducibles. There is no rational root (a rational root would be an integer factor of 12, and they are not roots), so there is no linear factor. To rule out two quadratic irreducible factors over Q, consider the mod 5 irreducible factorization:

$$X^4 + 8X^2 + 12 \equiv (X-4)(X^3 + 4X^2 + X + 2) \mod 5$$

If $X^4 + 8X^2 + 12$ were a product of two quadratics over Q, it would be a product of two monic quadratics over Z, and compatibility with the mod 5 factorization above would force there to be at least two roots mod 5, which there are not. The cubic resolvent of $X^4 + 8X^2 + 12$ is $X^3 - 48X - 64$, Which is irreducible mod 5 and thus is irreducible over Q.

So the Galois group of $X^4 + 8X^2 + 12$ over Q has size divisible by 3 (mod 4).

So the Galois group is either A_4 or S_4 The determinant of $X^4 + 8X^2 + 12$

is $331776 = 576^2 = (576)^2$, a perfect square, so the Galois group is A_4.

References

1. D. Dummit and R. Foote, " Abstract Algebra " 3es ed Wiley, New York 2004.
2. S, Lang, " Algebra " revised 3rd ed. Springer - Verlag, New York, 2002.
3. Keith Conrad, " Galois group of cubics and quadratic polynomial " (not in char.2).
4. Kaplansy, " Field and Ring. " 2nd ed. Uny .of Chicago Press, Chicago.
5. http://citeseerx.ist.psu.edu/viewdoc/summary
6. https://www.researchgate.net/publication/257554592_On_the_Hughes-Kleinfeld_and_Knuth's_semifields_two-dimensional_over_a_weak_nucleus
7. http://www.ms.uky.edu/~sohum/ma561/notes/workspace/books/cubicquartic.pdf